UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/044,019	01/11/2002	Partha Bhattacharya	50325-0629	8175

29989 7590 05/28/2008

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
05/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/044,019	BHATTACHARYA ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 March 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *10,11,14-16 and 33-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *10,11,14-16 and 33-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the RCE filed on 3 March 2008.

2. Claims 10, 11, 14-16 and 33-48 are pending in the application.

3. Claims 10, 11, 14-16 and 33-48 have been rejected.

4. Claims 1-9, 12, 13, 17-32 and 49-52 have been cancelled.

Continued Examination Under 37 CFR 1.114

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3 March 2008 has been entered.

Response to Arguments

6. Applicant's arguments with respect to claims 10, 11, 14-16 and 33-48 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 10, 11, 33-41 and 45-48 are rejected under 35 U.S.C. 102(b) as being anticipated by Montague et al U.S. Patent No. 5,761,669 (hereinafter Montague).

As to claim 10, Montague discloses a method as recited, wherein identifying first sub-entries in a first access control list comprises:

> identifying a dimensional range and a policy action for each entry in the first access control list (i.e. In FIG. 18, examples of the relationships listed in FIG. 12 for the inheritance attributes indicated by the inheritance flags, for existing and requested access inheritance are shown. Thus, for example, a Disjoint inheritance relationship occurs if the requested access inheritance does not include any inheritance flags and the existing inheritance has both the CI and OI inheritance flags set. In the example shown for the Equal inheritance relationship, the OI inheritance flag is set in both the requested access inheritance and the existing access inheritance for the entity; the inclusion of the NP flag in the existing access inheritance for the entity is ignored. The examples for the Subset and Superset relationships are self-evident. For the example shown to illustrate the Overlap relationship, the requested access inheritance flag is set for CI, which affects the container and all sub containers. The existing access inheritance has the OI

inheritance flag set, indicating that the inherited access permissions apply to the container and its immediately contained objects. Thus, the overlap between the requested access inheritance and the existing access inheritance is on the container, which is common to both) [column 17, lines 5-25];

identifying all overlapping dimensional ranges in the first access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the first access control list overlap (i.e. Perhaps the most extensive action required to complete the merger of an action control request with the ACL occurs when the appropriate action is identified in FIG. 14 by number 6. For example, if Donna is requested to have Read/Write permissions to a container MyFiles and to its sub objects, and if an existing ACE within the ACL denies Donna Write/Create Children permissions for Everything relative to the container MyFiles, the inheritance attribute requested overlaps with the existing inheritance attribute. Further, the requested access permissions that would grant Donna Read/Write permissions to the container MyFiles and its sub objects overlaps with the existing Denial of Write/Create Children. The fifth column of inheritance relationships under Overlap applies, and the fifth row of permissions relationships labeled Overlap intersect in a cell that includes action number 6) [column 18, lines 14-29];

identifying all non-overlapping dimensional ranges in the first access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the first access control list that do not overlap

dimensional ranges of other entries in the first access control list [column 17, lines 5-25];

identifying a policy action for each identified overlapping dimensional range in the first access control list [column 17, lines 5-25]; and

identifying a policy action for each identified non-overlapping dimensional range of the first access control list [column 17, lines 5-25].

As to claims 11 and 41, Montague discloses as recited, wherein identifying second sub-entries in a second access control list comprises:

identifying a dimensional range and a policy action for each entry in the second access control list [column 17, lines 5-25];

identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the second access control list overlap [column 17, lines 5-25];

identifying all non-overlapping dimensional ranges in the second access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list [column 17, lines 5-25];

identifying a policy action for each identified overlapping dimensional range of the second access control list [column 17, lines 5-25]; and

identifying a policy action for each identified non-overlapping dimensional range of the second access control list [column 17, lines 5-25].

As to claim 33, Montague discloses a method of comparing access control lists to configure a security policy on a network, the method comprising the computer-implemented steps of:

subtracting two entries among multiple first access control entries in a first access control list from each other (i.e. the relationship between an access control request 254 that is created by a trustee at a workstation 250 to modify the permissions for an entity, producing an appropriate ACE in an ACL 256, which is maintained on a server 252. In the example shown in this FIG., access control request 254 is a request to grant Write permissions to a specific group/individual, for a particular entity, such as a file. To merge this access control request with the existing ACEs maintained in ACL 256, the operating system searches the ACL to identify account IDs matching the specific group/individual account ID corresponding to the name of the individual/group included in the access control request. In this example, two ACEs are found with the same account ID, the first granting Read permissions to the entity and the second granting Delete permissions to the entity. Since the entity is simply a file, and not a container, inheritance attributes are not involved in merging the access control request with the ACL. As a result, as shown in ACL 256', the access control request is merged into the ACL, producing ACEs 258', the first of which grants Read/Write permissions to the account ID for the specific group/individual in the request, and

the second granting Delete/Write permissions to the file for the specific group/individual specified by the account ID. Any other ACEs 260 on the entity are not affected by the grant of the request) [column 15, lines 28-52];

determining, from results of subtracting the two entries among the multiple first access control entries in the first access control list from each other, a set of non-overlapping representation for dimensional ranges covered by the two entries among the multiple first access control entries in the first access control list [column 15, lines 28-52];

identifying, based on the set of non-overlapping representation, one or more first sub-entries in the first access control list [column 15, lines 28-52]; and

programmatically determining whether the first access control list is functionally equivalent to a second access control list by determining whether each of the first sub-entries in the first access control list is equivalent to or contained by one or more entries of multiple second access control entries the second access control list [column 15, lines 28-52].

As to claims 34, 38 and 46, Montague discloses determining that the first access control list is functionally equivalent to the second access control list in response to a determination that each of the first sub-entries is equivalent to or contained by one or more entries of the second access control list [column 15, lines 28-52].

As to claims 35, 39 and 47, Montague discloses a method as recited, further comprising:

identifying second sub-entries in the second access control list, wherein the second sub-entries identified from the second access control list comprise (i) disjoint entries of the second entries or (ii) overlapping sections identified from the second entries or (iii) non-overlapping sections identified from the second entries [column 16, lines 32-43]; and

wherein determining whether each of the first sub-entry in the first access control list is equivalent to or contained by one or more entries of the second access control list includes determining whether the each of the first sub-entries in the first access control list is equivalent to or contained by one or more of the second sub-entries identified from the second control list [column 16, lines 32-43].

As to claim 36, Montague discloses a computer readable medium for comparing access control lists to configure a security policy on a network, the computer readable medium carrying instructions for performing the steps of:

subtracting two entries among multiple first access control entries in a first access control list from each other (i.e. the relationship between an access control request 254 that is created by a trustee at a workstation 250 to modify the permissions for an entity, producing an appropriate ACE in an ACL 256, which is maintained on a server 252. In the example shown in this FIG., access control request 254 is a request to grant Write permissions to a specific group/individual, for a particular entity, such as a file. To merge this access control request with the

existing ACEs maintained in ACL 256, the operating system searches the ACL to identify account IDs matching the specific group/individual account ID corresponding to the name of the individual/group included in the access control request. In this example, two ACEs are found with the same account ID, the first granting Read permissions to the entity and the second granting Delete permissions to the entity. Since the entity is simply a file, and not a container, inheritance attributes are not involved in merging the access control request with the ACL. As a result, as shown in ACL 256', the access control request is merged into the ACL, producing ACEs 258', the first of which grants Read/Write permissions to the account ID for the specific group/individual in the request, and the second granting Delete/Write permissions to the file for the specific group/individual specified by the account ID. Any other ACEs 260 on the entity are not affected by the grant of the request) [column 15, lines 28-52];

determining, from the results of subtracting the two entries among the multiple first access control entries in the first access control list from each other, a set of non-overlapping representation for dimensional ranges covered by the two entries among the multiple first access control entries in the first access control list [column 15, lines 28-52];

identifying, based on the set of non-overlapping representation, one or more first sub-entries in the first access control list [column 15, lines 28-52]; and

programmatically determining whether the first access control list is functionally equivalent to a second access control list by determining whether

each of the first sub-entries in the first access control list is equivalent to or contained by one or more entries of multiple second access control entries in the second access control list [column 15, lines 28-52].

As to claim 37, Montague discloses a policy server communicatively coupled to security devices in a network to configure a security policy on a network, the policy server comprising:

a processor [column 5, lines 17-32];

a network interface that communicatively couples the processor to the network to receive flows of packets therefrom [column 5, lines 17-32];

a memory [column 5, lines 17-32]; and

sequences of instructions in the memory which, when executed by the processor, cause the processor to carry out the steps of:

subtracting two entries among multiple first access control entries in a first access control list from each other (i.e. the relationship between an access control request 254 that is created by a trustee at a workstation 250 to modify the permissions for an entity, producing an appropriate ACE in an ACL 256, which is maintained on a server 252. In the example shown in this FIG., access control request 254 is a request to grant Write permissions to a specific group/individual, for a particular entity, such as a file. To merge this access control request with the existing ACEs maintained in ACL 256, the operating system searches the ACL to identify account IDs matching the specific group/individual account ID corresponding to the name of the individual/group included in the access control request. In this example, two ACEs are found with the same account ID, the first

granting Read permissions to the entity and the second granting Delete permissions to the entity. Since the entity is simply a file, and not a container, inheritance attributes are not involved in merging the access control request with the ACL. As a result, as shown in ACL 256', the access control request is merged into the ACL, producing ACEs 258', the first of which grants Read/Write permissions to the account ID for the specific group/individual in the request, and the second granting Delete/Write permissions to the file for the specific group/individual specified by the account ID. Any other ACEs 260 on the entity are not affected by the grant of the request) [column 15, lines 28-52];

determining, from the results of subtracting the two entries among the multiple first access control entries in the first access control list from each other, a set of non-overlapping representation for dimensional ranges covered by the two entries among the multiple first access control entries in the first access control list [column 15, lines 28-52];

identifying, based on the set of non-overlapping representation, one or more first sub-entries in the first access control list [column 15, lines 28-52]; and

programmatically determining whether the first access control list is functionally equivalent to a second access control list by determining whether each of the first sub-entries in the first access control list is equivalent to or contained by one or more entries of multiple second access control entries in the second access control list [column 15, lines 28-52].

As to claims 40 and 48, Montague discloses a policy server as recited, wherein the instructions for performing identifying first sub-entries in a first access control list comprise:

> instructions for performing identifying a dimensional range and a policy action for each entry in the second access control list (i.e. In FIG. 18, examples of the relationships listed in FIG. 12 for the inheritance attributes indicated by the inheritance flags, for existing and requested access inheritance are shown. Thus, for example, a Disjoint inheritance relationship occurs if the requested access inheritance does not include any inheritance flags and the existing inheritance has both the CI and OI inheritance flags set. In the example shown for the Equal inheritance relationship, the OI inheritance flag is set in both the requested access inheritance and the existing access inheritance for the entity; the inclusion of the NP flag in the existing access inheritance for the entity is ignored. The examples for the Subset and Superset relationships are self-evident. For the example shown to illustrate the Overlap relationship, the requested access inheritance flag is set for CI, which affects the container and all sub containers. The existing access inheritance has the OI inheritance flag set, indicating that the inherited access permissions apply to the container and its immediately contained objects. Thus, the overlap between the requested access inheritance and the existing access inheritance is on the container, which is common to both) [column 17, lines 5-25];
>
> instructions for performing identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range

corresponding to where the dimensional ranges of entries in the second access control list overlap [column 17, lines 5-25];

instructions for performing identifying all non-overlapping dimensional ranges in the second access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list [column 17, lines 5-25];

instructions for performing identifying a policy action for each identified overlapping dimensional range in the second access control list [column 17, lines 5-25]; and

instructions for performing identifying a policy action for each identified non-overlapping dimensional range of the second access control list [column 17, lines 5-25].

As to claim 45, Montague discloses an apparatus for comparing access control lists to configure a security policy on a network, the apparatus comprising:

means for subtracting two entries among multiple first access control entries in a first access control list from each other (i.e. the relationship between an access control request 254 that is created by a trustee at a workstation 250 to modify the permissions for an entity, producing an appropriate ACE in an ACL 256, which is maintained on a server 252. In the example shown in this FIG., access control request 254 is a request to grant Write permissions to a specific group/individual, for a particular entity, such as a file. To merge this access

control request with the existing ACEs maintained in ACL 256, the operating system searches the ACL to identify account IDs matching the specific group/individual account ID corresponding to the name of the individual/group included in the access control request. In this example, two ACEs are found with the same account ID, the first granting Read permissions to the entity and the second granting Delete permissions to the entity. Since the entity is simply a file, and not a container, inheritance attributes are not involved in merging the access control request with the ACL. As a result, as shown in ACL 256', the access control request is merged into the ACL, producing ACEs 258', the first of which grants Read/Write permissions to the account ID for the specific group/individual in the request, and the second granting Delete/Write permissions to the file for the specific group/individual specified by the account ID. Any other ACEs 260 on the entity are not affected by the grant of the request) [column 15, lines 28-52];

means for determining, from the results of subtracting the two entries among the multiple first access control entries in the first access control list from each other, a set of non-overlapping representation for dimensional ranges covered by the two entries among the multiple first access control entries in the first access control list [column 15, lines 28-52];

means for identifying, based on the set of non-overlapping representation, one or more first sub-entries in the first access control list [column 15, lines 28-52]; and

means for programmatically determining whether the first access control list is functionally equivalent to a second access control list by determining whether each of the first sub-entries in the first access control list is equivalent to or contained by one or more entries of multiple second access control entries the second access control list [column 15, lines 28-52].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 14 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Montague U.S. Patent No. 5,761,669 as applied to claims 33, 37 and 45 above, and further in view of Brawn et al U.S. Patent No. 7,020,718 B2.

As to claims 14 and 42, Montague does not teach that identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a source address range and a destination address range for communication packets specified by each of the entries in the first access control list.

Brawn et al teaches identifying a source address range and a destination address range for communication packets specified by each of the entries in the first access control list [column 8 line 41 to column 9 line 2].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Montague so that a dimensional range and a policy action would have been identified for each entry in the first access control list that would have included identifying a source address range and a destination address range for communication packets specified by each of the entries in the first access control list.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Montague by the teaching of Brawn et al because an advantage includes providing a discontiguous address plan that allows thousands of discrete, different sized, and seemingly irregularly spaced address ranges to be accessed and identified by a small number of address and mask combinations. Another advantage includes providing an enterprise having a large complex network with a discontiguous network address plan configured to optimize for route advertisement, ACL entries, firewall configurations, and multiple network policies [column 6, lines 27-35].

9. Claims 15 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Montague U.S. Patent No. 5,761,669 as applied to claims 33, 37 and 45 above, and further in view of Mate et al U.S. Patent No. 7,020,718 B2.

As to claims 15 and 43, Montague does not teach that identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list.

Mate et al teaches identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list [column 11, lines 4-19].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Montague so that a dimensional range and a policy action would have been identified for each entry in the first access control list that would have included identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Montague by the teaching of Mate et al because it provides a method and system having fast search capabilities for classifying a plurality of types of data traffic and route lookup [column 3, lines 14-16].

10. Claims 16 and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Montague U.S. Patent No. 5,761,669 as applied to claims 33, 37 and 45 above, and further in view of Banginwar U.S. Patent No. 7,020,718 B2.

As to claims 16 and 44, Montague does not teach identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a communication protocol for communication packets specified by each of the entries in the first access control list.

Banginwar teaches identifying a communication protocol for communication packets specified by each of the entries in the first access control list [column 3, lines 18-46].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Montague so that a dimensional range and a policy action would have been identified for each entry in the first access control list that would have included identifying a communication protocol for communication packets specified by each of the entries in the first access control list.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Montague by the teaching of Banginwar because it enables a policy manage to communicate with the many devices connected to it [column 3, lines 47-54].

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/
Examiner, Art Unit 2131
/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131